P = Participant

I = Interviewer

I

So first of all, I don't know if you noticed, but there was some errors in the data that I gave you, unfortunately. That was not the tool that we're evaluating here, but it was the input data. The model had a few issues there. It's a bit unfortunate now, but it is how it is. Yeah, we'll see if that's an issue in your answers.

P

Okay, I didn't notice. Or maybe I did notice. I don't know. I cannot remember, actually.

I

Yeah, don't worry. I can look it up. So as a start, could you tell me your job description, please?

P

I'm an intern at [company]. I mainly work with machine learning and machine learning models and things and stuff currently for software security.

I

Okay.

P

But I'm not focused on software security.

I

So are you a developer?

P

Yes, yes. It's mostly developer. It could be sort of some other research intern kind of thing, but mostly it's developer.

I

Ok, sounds good. So can you put it into numbers? How many years of software development experience do you have?

P

Almost one. If you don't count my bachelor's degree, then it's just one.

I

Okay, that's fine. And security analysis, any experience, or…?

P

No, no.

I

Okay, thank you. So, on Monday you did two tasks manually first and two tasks where you had the tool output directly. If you compare that, was it easier in one of this, in any of these?

P

So you mean the ones where I had the tools output and then the ones that didn't have.

I

Yeah, exactly.

P

Yeah, it was much easier when I had the tool because I'm not very familiar with how should one approach a task like this. So having a tool with those specific outputs, it's easier to check the answer for the question I'm looking for.

I

Okay, all right. Do you think you were faster as well, or more efficient?

P

Yeah, in cases where there was evidence for the given question, in the tools output, I think I was faster because I could check whether I think the evidence is... whether the evidence holds or not. When there were no evidence or if something was a situation where we need the absence of something, it's harder to check. So in those cases, it's, I think, the same amount of effort, both manual and both with the tool, but when you have the evidence checking whether the evidence was, I think, faster. So it was faster in those cases.

I

Okay. Okay. So how exactly did you use the document that I gave you, the tool output? What did you do with it?

P

The HTML, you mean.

I

Yeah.

P

Yeah, I looked at it if... it was hard to work with it without having the dataflow graphs for me. So seeing visually the dataflow graph would have helped, but I looked at all the edges and nodes and in those cases, the evidences for edges. I don't know if you called it an evidence there, but the connection for an edge, but the tool thinks why there is a connection between the two nodes. Clicked on the links and looked at the relevant code snippets.

I

Okay, yeah.

P

I don't know if that's an answer for you on that.

I

Yeah, that's a good answer.

P

Should I go in more detail?

I

Oh no, I think that's fine. So let's say, did you trust the tool? So first of all, if you just see the verdict, the rule outcome, did you first trust it or did you have to double check? I mean, I know you did double check, but what was your trust in the output?

P

Yeah, yeah, I did double check it, especially in the last task where there were two parts.

I

Yeah.

P

Yeah, I think it's nice to check or nice to be able to check how the results came out. Check if all the edges are there or nodes there, what we expect. Or if… yeah, I think at first you don't trust the tool. Then you look at how it came to the conclusion.

I

Yeah. So over the course of the four tasks, did this change? So at the end, did you still not really trust it and double check or did your trust increase over the whole session on Monday?

P

I approached it with the same level of trust all throughout. So I checked always, I looked through all the parts in the document, not just the end result, try to see if everything is there or not.

I

Yeah, all right. Okay. You already said that you used the links to GitHub. Do you think they were enough to support the decisions basically? Was there anything missing?

P

It's a hard question to answer for me because I am not that familiar with all these frameworks. So in a few cases, I might have given a different answer, but that doesn't mean that I would have been correct in that case. So it might mean that I may be thinking that something is evidence, but I am not right. In one case, in the last task, if I remember correctly, I think one evidence was not correct. But that's also my intuition in that case. Sorry what was your question again? I might have gone to a different direction.

I

No, it's all good. If the links were enough, if there was information, I don't mean that you have to specifically for this, that you have to check if it's correct. But in general, this linking to GitHub and showing a small portion of the code, if this is enough for you to check.

P

Yeah, yes, that's enough. And it's great that it's very granular in a sense, that it links to not just only the file, but the concrete individual lines...

I

Yeah, okay.

P

...as well. Some properties doesn't have evidence. Does that mean they are labels which we have given or?

I

Yeah, basically. It's a heuristic, so that's not based on code. Yeah, exactly.

P

Okay.

I

So since you don't know Spring so much, did you then, did you Google, for example, the annotations or just by the…

P

[NODDING]

I

yeah, okay.

P

Yes, I looked up annotations, which seems sort of relevant or annotate or from the codes. I looked up all the annotations, what they mean and what they do.

I

Okay, I see. If we now just look at the structure of the HTML, so not the linking to code, but this step by step and listing all the nodes included / excluded and so on -- did you understand it directly, was it clear?

P

Yes, it was clear. Maybe the last one was harder to digest something.

I

With the logical operator?

P

No, in the third one...

I

Yeah.

P

...if something may be missing, but it's very clear other than that to understand in this table format, but yes that and what is not, yes.

I

Is there anything missing? Could you use any more information that we could put in there?

P

Other than the data flow diagrams, which I have already mentioned, I don't think there is anything else.

I

All right, okay. Now you didn't write the rules yourself, of course, the queries, but they're given on the top always -the statements and also in the Word document. Without me explaining it to you, do you still understand them directly? Can you read them and see okay, this is to understand what the rule is checking?

P

Yes, yes, absolutely.

I

Okay. Do you think with a bit of introduction to it, you could write these yourself?

P

Yeah, I'm somewhat confident, yes. If you know the rules, I mean the rules of the formalization, then yes.

I

Yeah, all right. Okay. Now, since you're not a security analyst, I don't know if the question makes much sense to you, but still I'm going to ask: do you think you could use such a tool -if we have a proper UI and everything- in your job? So if you do security analysis, do you think this would be helpful for you?

P

Yes, I think if I were a security analyst, this would be helpful.

I

Okay. Also as a software developer, do you see any use in there?

P

Yes, and mainly in the data flow diagrams, which we cannot see, but if I remember correctly, they are also generated by the tool. Or are they given by us?

I

No, it's a different tool that I have, but they are also automatically extracted.

P

Okay, that is also helpful, I think. And yeah, this is also helpful if you have a very large software, or many components in the architecture, it may be very helpful to check all these things. I don't know the scope of these properties, which can be automatically extracted. So I may not know what sort of properties I could check, other than these, which I have already seen. Yeah, that's what I can say.

I

Yeah, yeah, all right. So just to rephrase, basically for getting to know an application, this would be the kind of task that you would do with it.

P

Sorry, could you repeat the question?

I

No problem. I'm just rephrasing what you said. So you would use it to get to know an application that you don't know before or to get an overview?

P

Yes, it would be applicable for now.

I

Okay. All right, that's it already with my specific questions. Is there anything that you'd like to add? Anything that we didn't talk about?

P

In what extent does my inexperience affect the results in this case? So I think that the others are much more versed in how you approach questions like this or having a quick glance at a code like this, which you're unfamiliar with. My inexperience may have impacted this a lot.

I

Yeah, that's completely fine. First of all, you're not the only one. There were, I forgot who it was, but two others were also interns and not security analysts. And it's actually quite interesting as well for us, you know, to give it to someone who doesn't know how to usually do it. That's good insight for us. And yeah, of course, if you knew spring better, then probably you could give more insight and so on. But that's completely fine. Don't worry. I'm still happy to have your feedback. All right. If you don't have anything to add…

P

Yeah, a moment. Yeah, can the tool -- this may be a stupid question, but can the tool somehow guarantee that it has found all the connections between the nodes. Or in the last task where we look at whether encryption is used, can it -- could it give us an evidence of where in the code encryption is missing or it can just give us, "I couldn't find encryption, but you may have to look manually."

I

Yeah, it's a good question. So of course it's hard to show something that isn't there. In the case for encryption, we can do it a bit. So we can at least point to, for example, to the edge, the evidence of the edge. We can say, "this is where we found that there is a connection and we didn't find any encryption. So maybe somewhere here you have to look”. Also for some specific things, there is a certain place where that would have been. So for example, for encryption, we could point to some configuration file and then we say -I don't know- “there's no certificate here” or something like this. So a bit, yes, but it's hard. That's not easy. And for guaranteeing that we found all connections: no. That's even harder.

P

Okay, okay.

I

Yeah, what can you do? You can never be completely sure, right? Yeah, would be nice.

P

And is that theoretical aspects?

I

Exactly. Okay, all right. Then thanks a lot for your time and your feedback. I appreciate it. And yeah, I'll let you know via [name] if anything happens with this and then maybe get some insight.

P

Okay.

I

All right. Thanks a lot and have a nice day.

P

Have a nice day.

I

Bye.

P

Bye.